UNITED STATES DISTRICT COURT
for the
District of Massachusetts

COMBAT ZONE , Plaintiff v. DOES 1-84 , Defendant	No. 12-CV-30085-MAP

MOTION TO QUASH SUBPOENA

Now comes the Defendant, Doe Number 74, identified by IP Address 96.237.117.221, and hereby moves this Honorable Court, pursuant to Fed. R. Civ. P. 45 and 47 U.S.C. § 551, to enter an order quashing the subpoena issued by the Plaintiffs to Verizon for his/her personally identifying information.

I. BACKGROUND

Plaintiffs, Combat Zone Inc., have filed two lawsuits in Massachusetts alleging copyright violations by a total of 106 people. In both cases, Plaintiffs allege that a collection of John Doe Defendants used the bittorrent protocol (an electronic file transfer protocol) to download and share a film, the copyright to which Plaintiffs own. Bittorrent is a protocol, utilized by various programs and applications, to transfer electronic files. Typically, a user will download a very small ".torrent" file from a website, or use a program to search for files available for download via the bittorrent protocol. In either case, once the user finds a .torrent file or network with the file he or she seeks to download, the bittorrent application will join a network of other users seeking to share the file. Such networks are called "swarms."

Each swarm is associated with one particular .torrent file, which itself is differentiated from other .torrent files by a unique identifier, known as a "hash" value. A hash value is a string of numbers and letters derived mathematically from information contained within the .torrent file. The hash value itself is irrelevant; its only purpose is to be a unique alphanumeric string which differentiates that .torrent file, and the swarm associated therewith, from all others.

Referenced within each .torrent file are a series of other electronic files, which can be of any size or type. These are the files sought ultimately to be downloaded by the users. According to the bittorrent protocol, the files referenced by the .torrent file are broken up into thousands of very small pieces. Those pieces are then exchanged by members of the swarm. The bittorrent protocol assumes that each member of the swarm will simultaneously download and upload these pieces with the other members of the swarm, although some bittorrent applications will permit users to disable the uploading function. Eventually, all members of the swarm accumulate a complete collection of those pieces, which the bittorrent application reassembles into complete files,.

The trading of these file pieces within the swarm is commonly coordinated by a "tracker" computer, which indexes members of the network and facilitates communication between them. In some cases, the function of the tracker is performed by the users' applications themselves, and no central tracker is required (this technology is called a "distributed hash table"). Members of the swarm are listed on the tracker computer by "IP Address" which identifies each user's internet connection and provides information necessary for other computers to communicate with the modem at that address. The modem, in turn, routes communications to any and all computers at that address which access the internet through that modem. Members of the swarm can come and go at any time, whether their collection of file pieces is complete or not. In the absence of a log maintained by the user's bittorrent application, there is no way of knowing which user downloaded from, or uploaded to, any other user. The process by which users choose other peers from whom to download pieces of the file is not

random, but is too contingent to be worked out after the fact, and it is by no means the case that each and every user both downloads from and uploads to each and every other user.

Pursuant to Plaintiffs' Emergency Ex-Parte Motion for Early Discovery" (document #7), Plaintiffs intend to identify the John Doe Defendants in this case by issuing subpoenas to the Internet Service Providers which serviced various internet connections that the Plaintiffs identified as participating in a bittorrent swarm which was allegedly sharing works, the copyright to which Plaintiffs own. Those subpoenas have now issued, and John Doe number 74 now moves to quash that subpoena.

II. STANDING

The constitutional minimum requirements for standing are an injury in fact (an invasion of a legally protected interest), which is concrete and particularized, and which injury is actual or imminent, not conjectural or hypothetical, and fairly traceable to the challenged action and likely rather than speculative that the injury is redressable by the court. See Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992). In this case, the injury which will follow directly and imminently from compliance with the challenged subpoena is the release of Defendant's private contact information. That contact information, as is discussed in section III(a) of this memorandum, is legally protected, and the injury anticipated can be redressed by action of this court. Accordingly, Defendant has met the minimum constitutional standard for standing.

There has been cited a shorthand rule that "a party has no standing to quash a subpoena served upon a third party, except as to claims of privilege relating to the documents being sought." See Liberty Media Holdings v. Swarm Sharing Hash File, 821 F. Supp. 2d 444, 450 (D. Mass. 2011). Such a statement of the general rule is incomplete. In its entirety, the shorthand rule states that "[o]rdinarily, a party does not have standing to challenge a subpoena issued to a nonparty unless the party claims some personal right or privilege in the information sought by the subpoena." United States v. Idema, 118 Fed. Appx. 740 (C.A.4 (N.C.) Jan. 4, 2005) (citing Hertenstein v. Kimberly Home Health Care,

Inc., 189 F.R.D. 620, 635 (D. Kan. 1999)); CHARLES ALLEN WRIGHT & ARTHUR MILLER, FEDERAL PRACTICE AND PROCEDURE 9A §§ 2495 (1995). In this case Defendant claims a personal right in the information that is sought and therefore has standing.

The right to anonymity is an important foundation of the right to speak freely. Indeed, "[a]nonymity is a shield from the tyranny of the majority. It . . . exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation — and their ideas from suppression — at the hand of an intolerant society." Mclntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995). Accordingly, courts have held that the identity of the owner of an internet connection is entitled to "limited First Amendment protection," which subjects subpoenas for that information to "somewhat heightened scrutiny." London-Sire Records, Inc. v. Doe 1, 542 F. Supp. 2d 153, 162-63 (2008).

In London-Sire Records, Inc. v. Doe 1, the United States District Court for the District of Massachusetts considered motions to quash on their merits, which were filed by similarly situated Defendants. Id. Similarly, standing to challenge a subpoena for the type of records sought by the subpoena at issue in this case is both assumed, and impliedly provided for, in 47 U.S.C. § 551. That provision requires cable operators to notify the subject of records sought to be disclosed, and to "provide the subscriber the opportunity to prohibit or limit such disclosure." 47 U.S.C. § 551(c)(2)(C)(i). Finally, such standing is even contemplated in Plaintiffs "Memorandum in Support of Plaintiffs' Emergency Ex-Parte Motion for Early Discovery," (document #7) in which Plaintiffs state "[t]he John Does' expectation of privacy, if any, is protected by allowing them 21 days to quash the subpoena."

Given that Defendants have raised a personalized injury in fact, which was acknowledged in the London-Sire case, and which would directly and imminently result from compliance with the subpoena in this case; and given that both 47 U.S.C. § 551 and the Plaintiffs in this case acknowledge the necessity of permitting Defendants in cases such as this to challenge the subpoena, Defendant in this

case should have standing to raise this objection.

III. ARGUMENT

Under Federal Rule of Civil Procedure 45, a court shall quash or modify a subpoena if it requires disclosure of privileged or other protected matter and no exception or waiver applies. Fed. R. Civ. P. 45(c). On a motion to quash a subpoena, the party requesting that the subpoena be quashed bears the burden of showing good cause "by specifically demonstrating that disclosure will cause a clearly defined and serious harm. The court balances the harm of disclosure against the harm to the other party of restricting discovery." London-Sire, supra at 162 (citing Anderson v. Cryovac, Inc., 805 F. 2d 1, 7-8 (1st Cir. 1986); Glenmede Trust Co. v. Thompson, 56 F. 3d 476, 483 (3d Cir. 1995)). Following Sony Music Entertainment Inc. v. Does 1-40, London-Sire adopted a five part balancing test in cases such as this one:

> (1) a concrete showing of a prima facie claim of actionable harm, (2) specificity of the discovery request, (3) the absence of alternative means to obtain the subpoenaed information, (4) a central need for the subpoenaed information to advance the claim, and (5) the party's expectation of privacy.
>
> London-Sire, supra at 164 (following Sony Music Entertainment Inc. v. Does 1-40, 326 F. Supp. 2d 556 (S.D.N.Y. 2004))

a. Defendant's Right to Privacy and Anonymity is Legally Protected, and Disclosure Would Constitute Actionable Harm

"The first factor ensures that the [Plaintiffs] cannot pierce the defendants' anonymity based on an unsupported or legally insufficient pleading," and requires that the Plaintiffs (a) assert a claim upon which relief can be granted, (b) proffer sufficient evidence that, if credited would support a finding in their favor on all facts essential to their claim, and (c) set forth "concrete" allegations, in the sense that they are grounded in allegations of a specific act of infringement. London-Sire, supra at 164-65.

The substantive allegations made in this matter are contained in the affidavit of Jon Nicolini ("Nicoloni Affidavit) (document #1, attachment #2) and Exhibit A associated with the complaint in this

case ("Exhibit A") (document #1, attachment # 2). Exhibit A, lists IP Addresses and timestamps, which are explained by the Nicolini affidavit. In paragraphs 26 through 32, the Nicolini affidavit explains that the investigative company "CEG" locates IP Address which "are active members of the swarm," and "downloads a portion of the copy of the accused file," meanwhile logging the data set forth in Exhibit A. Allegedly, CEG downloads a complete copy of the accused file from the swarm twice, but at no point in the Nicolini affidavit is it alleged that a complete file is downloaded entirely from the IP Address which is logged and produced in Exhibit A. Indeed, doing so would be entirely contrary to the structure of the bittorrent protocol.

Essentially, then, the Nicolini affidavit asserts facts sufficient to conclude that, as it states, "at least one computer at each of the respective IP addresses listed in Exhibit A of the Combat Zone Inc. Complaint" was an "active member[]" of the swarm. In this sense, an "active member[]" appears to amount to an IP address from which CEG was able to download a "portion of the copy of the accused file." See Nicolini Affidavit, Par. 26. Notably, the Nicolini affidavit describes procedures designed to confirm that it is possible to download a completed file (twice) from the swarm (by downloading a complete copy and viewing the resulting file) but does not allege that any such procedures are employed to verify the data being received from the IP address included in Exhibit A. Nor does the Nicolini affidavit explain how much of the file is downloaded by CEG, so that in this case there is no way of knowing whether Defendant is alleged to have transmitted 100% of the accused file or .001% of the accused file to CEG.

The portion of the accused file either transmitted or possessed by the Defendant is of crucial importance because the Copyright Act provides for an action only for actual distribution, and not for merely attempted copyright infringement. See London-Sire, supra at 166-69; See also Venegas-Hernandez v. Asociacion de Compositores y Editores de Musica Latinoamericana, 424 F.3d 50 (1st Cir. 2005); In re Napster, Inc. Copyright Litigation, 377 F. Supp. 2d 796 (N.D.Cal. May 31, 2005). Indeed,

an amendment to the Copyright Act which would have provided for precisely such an 'attempted copyright infringement' was proposed in the Intellectual Property Protection Act of 2007 but never adopted. Intellectual Property Enforcement Act of 2007, 110th Congress, 2007–2009. Therefore, for Plaintiffs to sufficiently and concretely allege a violation of the Copyright Act, they must allege that an actual transfer of the file itself, and not an unspecified portion thereof, in fact took place. That allegation is absent from either the complaint, or the Nicolini affidavit, and without that allegation, the first of the Sony Music factors ought to weigh in favor of Defendant's motion to quash the subpoena.

Nor does the Nicolini affidavit specify which user(s) provided the data constituting the two completed downloads that were verified by CEG, making the inference drawn with regard to Plaintiffs second count (contributory infringement) pure speculation, particularly in light of the fact that the dates on which the various John Doe Defendants listed in Exhibit A were observed as "active members" of the swarm range from January 22 to March 25 of 2012. In short, to the extent that Plaintiffs allege contributory infringement in addition to actual infringement, those claims fall far short of the concrete specificity described by the London-Sire case, and the first factor ought to weigh in favor of Defendant's motion to quash.

b. Factors Two Through Four Are Uninstructive

"The second, third, and fourth factors in the Sony Music test are designed to ensure that the subpoena is appropriate to the Plaintiffs' needs, their allegations, and the preliminary evidence they have presented. The court weighs '(2) specificity of the discovery request, (3) the absence of alternative means to obtain the subpoenaed information, [and] (4) a central need for the subpoenaed information to advance the claim.'" London-Sire, supra at 177-78.

In London-Sire, the court faced a similar subpoena for records of an internet subscriber who the Plaintiffs in that case alleged had downloaded music in violation of their copyright. Id. The court observed that "[m]ore than one computer may be placed under a single IP number. Thus, it is possible

that the ISP may not be able to identify with any specificity which of numerous users is the one in question. If that is the case, giving the Plaintiffs a long list of possible infringers would permit precisely the sort of fishing expedition the Sony Music test is designed to avoid." Id. at 178. Since that time, numerous other courts have similarly observed that an IP address alone is insufficient to identify a particular person, and could instead identify the owner of a connection used by anyone else with access to his or her wireless router. See, e.g., In Re: Bittorrent Adult Film Copyright Infringement Cases, Nos. 11-3995, 12-1147, 12-1150, and 12-1154, 2012 U.S. Dist. LEXIS 61447, at *8 (E.D.N.Y May 1, 2012).

The response of the London-Sire court was to limit the subpoena by ordering that:

> The ISP shall submit to the Court, under seal, the information requested by the Plaintiffs for its consideration in camera. For any IP address provided by the Plaintiffs for which the ISP is unable to determine, to a reasonable degree of technical certainty, the identity of the user, it shall submit a list of all such users and a brief statement explaining the difficulty in selecting among them the alleged infringer.
>
> The ISP shall simultaneously submit to the Court its terms of service agreement with its users, or, if it does not have a terms of service agreement, a statement to that effect.
>
> The submissions by the ISP shall be made no later than 14 days after service of the subpoena.
>
> The ISP shall not disclose to the Plaintiffs any information regarding the identities of the Defendants unless ordered to do so by this Court.
>
> London-Sire, supra at 180.

In effect, the court ordered that the information be submitted in camera to the court, for further consideration on the possibility of separating the relevant and probative information of the user who was responsible for the file transfer alleged, from the private and irrelevant information of the person who paid for the internet subscription. Without knowing what information the Internet Service Provider may be able to offer, Defendant does not know whether, or to what degree a similar order would assist the court in this case.

In any case, although the request itself may be as specific as is practicable for Plaintiffs, that degree of specificity remains entirely unrelated to the protection of the privacy interests against which it must be weighed. Requests for information which is both irrelevant to the issue of the person responsible for downloading Plaintiffs' copyrighted work, and which constitute private and protected information about Defendant, cannot be made any less harmful or irrelevant by making those requests more specific, except to the extent that those request are altered to request the information of the person who was actually using the computer to download Plaintiffs' copyrighted work (information which the internet service provider likely does not have). Accordingly, the second, third, and fourth factors of the Sony Music test are uninstructive on the issue of the degree to which the requests made by the subpoena are narrowly tailored, and should weigh neither in favor nor against Defendant's motion.

c. Defendant Maintains a Reasonable and Legitimate Expectation of Privacy

In contexts outside the realm of copyright law, courts have clarified that the question of the degree to which a person might hold a reasonable and legitimate expectation of privacy are governed both by whether the person had a subjective expectation of privacy and whether that subjective expectation of privacy is one that society is prepared to recognize as reasonable. See e.g. Kyllo v. United States, 533 U.S. 27, 33 (2001) (Fourth Amendment context). Where the question of reasonable expectations arises, the fact that those expectations might be mistaken is not necessarily dispositive. See Smith v. Maryland, 442 U.S. 735, 740 & n.5 (1979) ("[W]here an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a 'legitimate expectation of privacy' existed in such cases, a normative inquiry would be proper.").

Other cases in which courts have held that no such privacy interest exists (See, e.g., Liberty Media Holdings v. Swarm Sharing Hash File, 821 F. Supp. 2D 444, 450 & n.3 (D. Mass. 2011) are

founded upon two mistaken propositions. The first mistaken proposition is that the wrongdoing of the downloader somehow forfeits whatever privacy interest the Defendant might otherwise have enjoyed. It has been stated, for example, that "if an individual subscriber opens his computer to permit other, through peer-to-peer file-sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world." Sanchez v. Doyle, 257 F. Supp. 2d 266, 267 (D. Conn. 2003). This argument puts the cart before the horse, and assumes that the person whose information is sought in relation to the subpoena is in fact the person who chose to open his or her computer to the world. As previously discussed, there is no necessary relation between the person who owns the internet connection and the person who may have chosen to expose their own computer to the world. The argument also short-circuits the entire issue by giving the Plaintiffs the power to generate the only evidence necessary to overcome a Defendant's privacy interest -- a mere allegation of copyright infringement. If the allegation alone is enough to overcome the privacy interest acknowledged in London-Sire, then that privacy interest is thereby rendered purely academic.

The second mistaken proposition which has been offered in similar cases is that "[i]nternet subscribers do not have a reasonable expectation of privacy in their subscriber information - including name, address, phone number, and email address - as they have already conveyed such information to theirs ISPs." See, e.g., First Time Videos, LLC v. Does 1-500, 276 F.R.D. 241 (N.D. Ill. Aug. 9, 2011). Verizon's Privacy Policy states that "personally identifying" information is disclosed only " to the extent reasonably necessary for them to perform work on our behalf." About Verizon – Privacy Policy, http://www22.verizon.com/about/privacy/policy/ (Last Viewed June 25, 2012). The fact that Verizon also acknowledges in its policy that it is bound by law to comply with legal process cannot be cited for the proposition that Defendants lack an interest in privacy without at the same time presuming the appropriateness of the subpoena which is being challenged by this motion. An interest and belief in

privacy cannot be dispelled by capitulation to a true statement of fact that, if compelled by court order, Verizon must turn over the information as commanded. See Smith v. Maryland, 442 U.S. 735, 740 & n.5 (1979).

Meanwhile, there is every reason to believe that an internet service customer does expect his or her identifying information to remain private, and that belief appears to have the sanction of law. Besides the Verizon "Family of Companies" described in its privacy policy, Verizon tells its customers that it will not share "information that individually identifies [its] customers" -- which is precisely what the Plaintiffs seek in the challenged subpoena. About Verizon – Privacy Policy, http://www22.verizon.com/about/privacy/policy/ (Last Viewed June 25, 2012).

Defendant's expectation of privacy is further supported by statute enacted at 47 U.S.C. § 551, as described below in Section IV of this memorandum.

Based on the Verizon privacy policy, and the support it finds in 47 U.S.C. § 551, Defendants have a reasonable expectation of privacy as described in the Sony Music test. Accordingly, the fifth factor of the Sony Music test should weigh in favor of Defendant's motion to quash.

IV. Plaintiffs' SUBPOENA IS BARRED BY 47 U.S.C. § 551

47 U.S.C. § 551 both prohibits the disclosure sought in this case, and simultaneously illustrates the widely-held sentiment that such information is private. §551 provides that (except as provided within that statute) a "cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator." 47 U.S.C. § 551(c)(1). §551(c)(2), in turn provides four exceptions to the general rule: (A) for legitimate business activity related to a cable service; (B) upon a showing of "clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity," (C) after notifying the user, and after the user has an opportunity to challenge the

disclosure; and (D) to a government entity (inapplicable in this case).

As Plaintiffs are neither a government entity nor a cable service, the Plaintiffs in this case must be proceeding under exception C. Exception C, however, is limited, and permits disclosure only "if . . . the disclosure does not reveal, directly or indirectly, the – (i) extent of any viewing or other use by the subscriber of a cable service or other service provided by the cable operator, or (ii) the nature of any transaction made by the subscriber over the cable system of the cable operator." 47 U.S.C. § 551(c)(2)(C)(i)-(ii). Plaintiffs' sole purpose (as it is stated in Plaintiffs motion for expedited discovery), in seeking to obtain the identifying information of a party to a file transfer which the Plaintiffs have already monitored, is to indirectly reveal the extent of use by the subscriber, and the nature of the transaction monitored. As such, the Plaintiffs' purpose, and the effect of permitting compliance with Plaintiffs' subpoena, is directly contrary to both the intent and the plain language of the statute, and on that basis, the subpoena in this case should be quashed.

V. CONCLUSION

Defendants have standing in this case as provided in 47 U.S.C. § 551, and conceded by the Plaintiffs in their Memorandum in Support of Plaintiffs' Emergency Ex-Parte Motion for Early Discovery. Based on the balance of interests, described in Sony Music and London-Sire, Defendant's interest in privacy and anonymity are entitled to limited first amendment protection, which interest is not outweighed by Plaintiffs' need for discovery of the potentially irrelevant information of the name of the person who pays for the internet connection. Furthermore, the information sought by Plaintiffs is explicitly barred, under these circumstances, by 47 U.S.C. § 551(c)(2)(C)(i)-(ii) as disclosing that information would indirectly lead to the disclosure of the extent of use by the subscriber. For those reasons, Defendant respectfully prays this Honorable Court quash the subpoena issued to Verizon for subscriber information associated with IP Address 96.237.117.221 on 1/31/2012 at 5:55:50 AM GMT, and for such other and further relief as the Court deems appropriate.

Respectfully submitted,
Defendant
By his Attorney,

/s/ Edward R. Molari
Edward R. Molari, Esq.
BBO#: 675771
185 Devonshire St., STE 302
Boston, MA 02110
Phone: (617) 942-1532
Fax: (815) 642-8351
Email: edward@molarilaw.com

Dated: Thursday, June 28, 2012

CERTIFICATE OF SERVICE

I hereby certify that on Thursday, June 28, 2012, the foregoing document, together with all documentary exhibits was filed through the ECF system and electronically sent to all registered participants as identified on the Notice of Electronic Filing as of the day and time of filing.

Dated: Thursday, June 28, 2012 Signature: /s/ Edward R. Molari